

20191011272

СОБРАНИЕ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на членот 75, ставови 1, 2 и 3 од Уставот на Република Северна Македонија, претседателот на Република Северна Македонија и претседателот на Собранието на Република Северна Македонија издаваат

УКАЗ ЗА ПРОГЛАСУВАЊЕ НА ЗАКОНОТ ЗА ЕЛЕКТРОНСКИ ДОКУМЕНТИ, ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА И ДОВЕРЛИВИ УСЛУГИ (*)

Се прогласува Законот за електронски документи, електронска идентификација и доверливи услуги (*),

што Собранието на Република Северна Македонија го донесе на седницата одржана на 16 мај 2019 година.

Бр. 08-2894/1
16 мај 2019 година
Скопје

Претседател на Република
Северна Македонија,
Стево Пендаровски, с.р.

Претседател
на Собранието на Република
Северна Македонија,
м-р **Talat Xhaferi**, с.р.

ЗАКОН ЗА ЕЛЕКТРОНСКИ ДОКУМЕНТИ, ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА И ДОВЕРЛИВИ УСЛУГИ (*)

І. ОПШТИ ОДРЕДБИ

Предмет

Член 1

(1) Со овој закон се уредува создавањето, складирањето и обработката на електронските документи, електронската идентификација и доверливите услуги.

(2) Со овој закон се уредува и употребата на електронските документи, електронскиот потпис и електронскиот печат и електронските доверливи услуги во управни и судски постапки.

(3) Предмет на уредување на овој закон се условите под кои се признаваат средствата за електронска идентификација издадени на физички и правни лица кои спаѓаат во рамки на регистрирана или признаена шема за електронска идентификација.

Цел

Член 2

(1) Целта на овој закон е обезбедување на безбедност на средствата за електронска идентификација и безбедност при обезбедување доверливи услуги.

* Со овој закон се врши усогласување со Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за електронска идентификација и доверливи услуги за електронски трансакции во внатрешниот пазар и за укинување на Директива 1999/93/ЕЗ со CELEX број 32014R0910

(2) Цел на овој закон е уредување на електронските потписи, електронските печати, електронските временски жигови, електронските документи, услугите за електронска препорачана достава, услугите за проверка на автентичност на веб страници, како и зачувувањето на електронскиот потпис или печат и нивна валидација.

Дефиниции

Член 3

(1) Одделни изрази употребени во овој закон, го имаат следново значење:

1) формат на електронски податоци се податоци создадени во електронска форма, погодни за електронска обработка и пренос преку електронски комуникациски системи;

2) електронска трансакција е активност помеѓу две или повеќе страни, којашто се извршува по електронски пат;

3) електронски документ е секоја содржина складирана во електронска форма, особено текстуални или звучни, визуелни или аудио-визуелни записи;

4) производ е хардвер, софтвер или соодветните компоненти на хардвер или софтвер предвидени да се користат при обезбедување на доверливи услуги;

5) интероперабилност е способноста на два или повеќе системи или нивните компоненти за размена на податоци и олеснување на заедничката употреба на податоци и знаење;

6) јавен орган е државен орган, орган на државната управа, единица на локалната самоуправа, јавни претпријатија, установи, организации и правни лица на кои им се делегирани јавни овластувања во согласност со законодавството на Република Северна Македонија;

7) автентикација е електронски процес кој овозможува електронска идентификација на физичко или правно лице или кој овозможува потврдување на потеклото и интегритетот на податоците во електронска форма;

8) податоци за идентификација на лица се збир на податоци врз основа на кои единствено е можно да се идентификува идентитетот на правно лице, физичко лице или овластено лице на правно лице;

9) електронска идентификација е процес на користење на податоци за идентификација на лица во електронска форма кои на уникатен начин го претставуваат физичкото или правно лице или овластено лице на правно лице;

10) средства за електронска идентификација се материјални или нематеријални средства кои содржат податоци за идентификација на лица, а се користат за автентикација кај електронски услуги;

11) издавач на средство за електронска идентификација е правно лице кое ги исполнува условите утврдени во овој закон за издавачи на средство за електронска идентификација;

12) шема за електронска идентификација е систем за електронска идентификација според кој средствата за електронска идентификација се издаваат на физички или правни лица или овластено лице на правно лице;

13) доверлива услуга е електронска услуга при електронски трансакции, која се состои од:

- создавање, валидација и верификација на електронски потписи, електронски печати или електронски временски жигови, услуги за електронска препорачана достава, како и сертификати поврзани со овие услуги или

- создавање, валидација и верификација на сертификати за автентичност на веб страници или

- зачувување на електронски потписи, печати или потврди поврзани со овие услуги.

Доверливите услуги може да бидат неквалификувани и квалификувани.

14) давател на доверлива услуга е правно лице кое обезбедува една или повеќе доверливи услуги;

15) засегната страна е физичко или правно лице кое има правен интерес од електронска идентификација или доверливи услуги;

16) квалификувана доверлива услуга е вид на доверлива услуга што ги исполнува условите утврдени со овој закон кои се однесуваат за квалификувана доверлива услуга;

17) давател на квалификувана доверлива услуга е давател на доверлива услуга кој обезбедува една или повеќе квалификувани доверливи услуги и чиј статус на давател на квалификувана доверлива услуга е доделен од страна на министерот за информатичко општество и администрација со регистрација во Регистарот на шеми за електронска идентификација и на доверливи услуги.

Давател на квалификувана доверлива услуга е правно лице на кое му се доделени јавни овластувања, согласно со одредбите од овој закон;

18) електронски потпис е збир на податоци во електронска форма кој е придружен кон или е логички поврзан со други податоци во електронска форма и кој потписникот го користи за потпишување;

19) електронски печат е збир на податоци во електронска форма кој е придружен кон или е логички поврзан со други податоци во електронска форма, со што се обезбедува сигурност на потеклото и интегритетот на придружените или поврзаните податоци;

20) податоци за изработка на електронски потпис се единствени податоци кои се користат од страна на потписникот за создавање на електронски потпис;

21) податоци за валидација се податоците кои се користат за валидација на електронски потпис или електронски печат;

22) сертификат за електронски потпис е електронска потврда која ги поврзува податоците за валидација на електронскиот потпис со физичко лице и која го потврдува најмалку името или псевдонимот на тоа лице;

23) сертификат за електронски печат е електронска потврда која ги поврзува податоците за валидација на електронскиот печат со правното лице и која го потврдува името на правното лице;

24) потписник е физичко лице кое создава електронски потпис;

25) создавач на електронски печат е правно лице кое создава електронски печат и истото во смисла на овој закон е определено и како запечатувач;

26) средство за создавање на електронски потпис или електронски печат е техничко средство, односно конфигуриран софтвер или хардвер, што се користи за создавање електронски потпис или електронски печат;

27) валидација е постапката за проверка и потврдување дека електронскиот потпис или електронскиот печат се валидни;

28) напреден електронски потпис е електронски потпис кој ги исполнува условите утврдени со овој закон кои се однесуваат за напреден електронски потпис;

29) квалификуван електронски потпис е напреден електронски потпис кој е создаден од средство за изработка на квалификуван електронски потпис и кој се заснова на квалификуван сертификат за електронски потпис;

30) средства за создавање на квалификуван електронски потпис или печат се средства кои ги исполнуваат условите утврдени во овој закон, а кои се однесуваат на средства за создавање на квалификуван електронски потпис или печат;

31) квалификуван сертификат за електронски потпис е сертификат за електронски потпис издаден од давател на квалификувана доверлива услуга и кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за електронски потпис;

32) напреден електронски печат е електронски печат кој ги исполнува условите утврдени со овој закон кои се однесуваат за напреден електронски печат;

33) квалификуван електронски печат значи напреден електронски печат кој е изработен од средство за изработка на напреден електронски печат и кој се заснова на квалификуван сертификат за електронски печат;

34) податоци за изработка на електронски печат се единствени податоци кои се користат од страна на создавачот на електронски печат со цел создавање на електронски печат;

35) квалификуван сертификат за електронски печат е сертификат за електронски печат издаден од давател на квалификувана доверлива услуга и ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за електронски печат;

36) сертификат за автентичност на веб страница е потврда што овозможува да се потврди автентичноста на дадена веб страница и ја поврзува веб страницата со физичкото или правното лице на кое му е издаден сертификатот за автентичност на веб страница;

37) квалификуван сертификат за автентичност на веб страница е сертификат за автентичност на веб страница издадена од давател на квалификувана доверлива услуга и кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за автентичност на веб страница;

38) електронски временски жиг е збир на податоци во електронска форма кој поврзува други податоци во електронска форма со конкретно време и претставува доказ дека поврзаните податоци постоеле во конкретниот момент;

39) квалификуван електронски временски жиг е електронски временски жиг кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван електронски временски жиг;

40) електронска препорачана достава е услуга која овозможува пренос на податоци помеѓу трети страни по електронски пат и обезбедува доказ во врска со преносот на податоците, вклучувајќи доказ за испраќање и примање на податоците, а притоа го заштитува преносот на истите од ризикот од загуба, кражба, оштетување или недозволените измени;

41) квалификувана електронска препорачана достава е услуга за електронска препорачана достава што ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификувана електронска препорачана достава;

42) конверзија е промена на формата или форматот на документот од една форма или формат во друга форма или формат, така што содржината на документот останува непроменета;

43) дигитализација е процес на конверзија на документ чијашто форма не е електронска во дигитализиран документ;

44) дигитализиран документ е електронски документ што е создаден со дигитализација на оригинални документи во писмена форма;

45) електронско складирање на документи е чување на документи во електронска форма, за кои е точно определено времето на чување на тие документи, соодветно на времето на чување на документите во печатена форма, за кои времето на складирање е потврдено со електронски временски жиг;

46) квалификувано електронско складирање на документи е чување на електронски документи, кои при нивното складирање се потврдени со квалификуван електронски потпис или печат и квалификуван временски жиг;

47) ознака за доверба на доверлива услуга е ознака којашто е јасно препознатлива и којашто јасно упатува дека доверливата услуга ја обезбедува конкретен давател на доверлива услуга;

48) ознака за доверба на квалификувана доверлива услуга е ознака којашто е јасно препознатлива и којашто јасно упатува дека квалификуваната доверлива услуга ја обезбедува конкретен давател на квалификувана доверлива услуга;

49) тело за оценување на сообразноста е правно лице акредитирано да врши проценка на усогласеноста за исполнетост на услови кои се однесуваат на давател на квалификувана доверлива услуга и на квалификувани доверливи услуги кои истиот ги обезбедува;

50) лабораторија за тестирање е правно лице акредитирано да врши проценка на усогласеност на средствата за издавање на електронска идентификација, електронски потписи или електронски печати со условите определени со овој закон.

(2) Изразите што се употребуваат во овој закон чие значење не е дефинирано во ставот (1) на овој член, имаат значење утврдено со друг закон.

Примена на законот

Член 4

(1) Одредбите од овој закон се применуваат и за спречување на перење на пари, преку идентификување на корисникот на доверливите услуги, потврдување на неговиот идентитет врз основа на обработка на документи, податоци или информации добиени од сигурен и независен извор, вклучувајќи и средства за електронска идентификација, соодветни доверливи услуги.

(2) Одредбите од овој закон кои се однесуваат на доверливи услуги не се применуваат во рамки на затворен систем или систем наменет за ограничена група на учесници, чијашто употреба може да се утврди со договор или со внатрешен акт, а кој систем нема влијание врз трети лица или не предизвикува обврски за трети страни надвор од тој систем.

Обработка и заштита на лични податоци

Член 5

(1) Давателот на доверлива услуга при обработката на личните податоци до кои има пристап во текот на вршењето на дејноста постапува согласно со прописите од областа на заштитата на личните податоци.

(2) При извршување на електронска трансакција, корисникот може да употреби и псевдоним, доколку користењето на псевдонимот кој е употребен не е во спротивност со одредбите од друг закон.

II. ЕЛЕКТРОНСКИ ДОКУМЕНТ

Правно дејство на електронскиот документ

Член 6

(1) Електронскиот документ има иста правна и доказна сила како и писмената форма на документот, согласно со закон.

(2) Електронскиот документ не може да се оспори како доказ во управна или судска постапка, само затоа што е создаден во електронски облик.

(3) Кога со закон е утврдена писмена форма на документите или актите, електронскиот документ се смета за документ или акт во писмена форма.

Создавање на електронски документ

Член 7

(1) Електронски документ се создава со користење на една или повеќе од достапните и употребливи информатички и комуникациски технологии, освен ако со друг закон поинаку не е уредено.

(2) Електронскиот документ како архивски материјал се создава во форма која ги исполнува условите утврдени во овој закон, а е погодна за подготовка за сигурносно електронско складирање.

Оригинал и копија

Член 8

(1) Секој умножен електронски примерок на конкретен електронски документ се смета за оригинал.

(2) Електронски документ создаден со дигитализација на изворниот документ чија првична форма не е електронска, се смета за копија на оригиналниот документ.

(3) Кога електронскиот документ е репродуциран во хартиена форма се смета за копија на оригиналниот документ.

Дигитализација на документи

Член 9

(1) Дигитализираниот документ ја има истата правна и доказна сила како оригиналниот документ, ако:

1) дигитализацијата на документот е извршена под надзор или од страна на:

- физичко лице или овластено лице на правно лице којшто го создал документот што е предмет на дигитализација или

- лица кои се овластени да ракуваат со документи во кои се содржани потписи, ракописи или записници, согласно со прописите од областа на архивското и канцелариското работење или

- лица кои се овластени со закон да го потврдат дигитализираниот документ и

2) идентичноста на дигитализираниот документ со оригиналниот документ е потврдена со квалификуван електронски печат или квалификуван електронски потпис на лицата од точка 1) на овој член или лицето на кое се пренесени надлежностите врз основа на кои е донесен документот.

Верификација на печатена форма на електронски документ

Член 10

Електронскиот документ репродуциран на кој било печатен медиум ја има истата правна и доказна сила како оригиналниот електронски документ, доколку:

1) умножувањето на електронскиот документ е извршено под надзор или од страна на физичко лице или овластено лице на правно лице кое го создало документот и

2) печатењето на документот е извршено на начин што идентичноста на електронскиот документ со печатениот документ се потврдува со своерачен потпис на физичко лице или овластено лице на правно лице.

III. ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

1. Шеми за електронска идентификација

Услови кои треба да ги исполнуваат шемите за електронска идентификација

Член 11

Шемите за електронска идентификација ги исполнуваат следните услови:

- 1) да вклучат потврда за податоците за идентификација на лицата на кои им се издадени средства за електронска идентификација, кои на единствен начин го определуваат правното или физичкото лице;
- 2) да обезбедат сигурност дека издавачот на средството за електронската идентификација обезбедува идентификациски податоци во рамките на средствата за електронска идентификација што соодветствуваат на лицето на кое му е издадено средството за електронска идентификација;
- 3) да ги исполнуваат условите за нивото на сигурност во кој е класифицирана шемата за електронска идентификација, од членот 13 од овој закон.

Согласност за идентификација

Член 12

Постапката за издавање на електронска идентификација се поведува по претходно барање на физичко или правно лице кое е субјект на идентификација пред издавач на средства за електронска идентификација освен ако со закон поинаку не е уредено.

Нивоа на сигурност на шемите за електронска идентификација

Член 13

Шемите за електронска идентификација се класифицирани според нивото на сигурност на средствата за електронска идентификација кои се издадени во рамките на таа шема и тоа:

- 1) ниско ниво на сигурност обезбедува ограничен степен на сигурност на бараниот или потврдениот идентитет на лицето и се карактеризира со упатување кон соодветни технички спецификации, стандарди и постапки, вклучувајќи и технички проверки, чија цел е намалување на ризикот од злоупотреба или промена на идентитетот;
- 2) значително ниво на сигурност обезбедува значителен степен на сигурност на бараниот или потврдениот идентитет на лицето и се карактеризира со упатување кон соодветните технички спецификации, стандарди и постапки, вклучувајќи и технички проверки, чија цел е значително да се намали ризикот од злоупотреба или промена на идентитетот и
- 3) високо ниво на сигурност обезбедува повисок степен на сигурност на бараниот или потврдениот идентитет на лицето отколку средствата за електронска идентификација со ниво на сигурност „значително“ и се карактеризира со упатување кон соодветни технички спецификации, стандарди и постапки, вклучувајќи и технички проверки, чија цел е спречување на злоупотреба или промена на идентитетот.

Регистар на даватели на доверливи услуги и на шеми за електронска идентификација

Член 14

(1) Давателот на доверлива услуга до Министерството за информатичко општество и администрација доставува барање за регистрација во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација (во натамошниот текст: Регистарот), кој го води Министерството за информатичко општество и администрација.

(2) Во Регистарот задолжително се регистрираат шемите за електронска идентификација кои ги употребуваат јавните органи.

(3) Во Регистарот по претходно поднесено барање од страна на јавниот орган или приватното правно лице може да се регистрираат и шеми за електронска идентификација кои се создадени од јавни органи и шеми кои се создадени од приватни правни лица.

(4) Шемите создадени од јавните органи се регистрираат во Регистарот врз основа на решение за регистрација донесено од страна на министерот за информатичко општество и администрација, а по претходно поднесено барање за регистрација на шема од страна на јавниот орган.

(5) Шемите создадени од приватни правни лица задолжително треба да одговараат на високо ниво за сигурност за да бидат регистрирани во Регистарот.

(6) Регистарот од ставот (1) на овој член особено ги содржи следните информации за давателот на доверлива услуга:

- име на правното лице,
- информации за контакт како што се: адреса, телефонски број и електронска пошта,
- видот на услуги што ги обезбедува издавачот на шемата за електронска идентификација,
- средствата за електронска идентификација кои се користат во рамки на шемата и
- нивото на сигурност.

(7) Во Регистарот се регистрираат и давателите на квалификувана доверлива услуга.

(8) Давателите на доверливи услуги и шемите за електронска идентификација може да бидат избришани од Регистарот, доколку:

- престанат да ги исполнуваат условите определени со овој закон,
- не бидат отстранети отстапувањата од овој закон по претходно укажување за отстранување на недостатоци во рокот утврден во решението за отстранување на неправилности издадено согласно со овој закон или
- во други случаи определени со закон за бришење на правни лица од евиденција на надлежен орган.

(9) Министерот за информатичко општество и администрација ја пропишува содржината и начинот на водење на Регистарот од ставот (1) на овој член, како и начинот на поднесување на барањето за регистрација, потребната документација како прилог кон барањето, образецот на барањето и начинот на објавување на податоците од Регистарот, во зависност од видот на доверливоста на услугата.

Употреба на шеми за електронска идентификација во електронска трговија и комуникација со јавен орган

Член 15

(1) За електронска идентификација на лицето кое води постапка пред јавен орган, задолжително се користи шема за електронска идентификација која е регистрирана во Регистарот од членот 14 од овој закон (во натамошниот текст: регистрирана шема за електронска идентификација).

(2) За електронска идентификација на лицето кое презема дејствија поврзани со активностите на приватниот сектор, вклучувајќи и електронска трговија, по сопствен избор може да користи регистрирана шема или шема за електронска идентификација која не е регистрирана во Регистарот од членот 14 од овој закон.

Одговорност за штета од употреба на регистрирани шеми за електронска идентификација

Член 16

(1) Издавачот на регистрирана шема за електронска идентификација е одговорен за штетата која може да настане поради тоа што шемата не ги исполнува условите од овој закон.

(2) Штетата настаната како последица на погрешно спроведената постапка за валидација е одговорност на странката што ја води постапката, ако штетата била предизвикана намерно или од небрежност.

(3) Товарот за докажување за настаната штета е на страна на лицето што истакнало побарување за надоместок на штета.

(4) Издавачот од ставот (1) на овој член е должен да биде осигуран од евентуална штета која може да ја предизвика.

(5) Најнискиот износ од осигурувањето од евентуалната штета предизвикана од издавачот ќе го пропишува министерот за информатичко општество и администрација.

Барање за утврдување на исполнетост на услови за нивоа на сигурност на шеми

Член 17

(1) Барањето за утврдување на исполнетост на услови за нивоа на сигурност на шеми е прилог кон барањето за регистрација во Регистарот од членот 14 од овој закон.

(2) Барањето од ставот (1) на овој член ги содржи следните информации:

1) начинот на докажување и верификација на идентитетот на физичко или правно лице кое бара издавање на средство за електронска идентификација;

2) начинот на издавање на средствата за електронска идентификација;

3) механизмите за автентикација, преку кои физичко или правно лице, користејќи ги средствата за идентификација, го потврдува својот идентитет на засегнатата страна;

4) условите што треба да ги исполнат останатите учесници вклучени во постапката за издавање средства за електронска идентификација;

5) техничките и безбедносните карактеристики на средствата за електронска идентификација што се издаваат во рамки на шемата;

6) технички и организациски мерки кои ги исполнува издавачот на средства за електронска идентификација со цел да се обезбеди интероперабилност на шемите за електронска идентификација во согласност со националните и меѓународните стандарди во оваа област;

7) извештај за ниво на сигурност на шемата за електронска идентификација од тело за оценување на сообразноста и

8) податоци за издавачот на шемата за електронска идентификација.

Безбедносни услови што треба да ги исполнат издавачите на шемите за електронска идентификација

Член 18

(1) Издавачот на шемата за електронска идентификација е должен да ги преземе потребните технички, физички и организациски мерки за управување со ризиците кои би можеле да го загорзат обезбедувањето на овие услуги на сигурен и безбеден начин.

(2) Техничките, физички и организациски мерки треба да обезбедат нивото на безбедност да одговара на нивото на ризик и предвиденото ниво на сигурност на шемата за електронската идентификација, земајќи ги предвид најновите достапни технолошки решенија, а особено мерките за спречување на безбедносни инциденти и за ограничување на штетните ефекти од можните инциденти, како и за информирање на засегнатите страни за несакани ефекти од безбедносни инциденти.

(3) Процедурите и стандардите за исполнетост на техничките, физички и организациски мерки за сигурност на шеми за електронска идентификација ги пропишува министерот за информатичко општество и администрација.

(4) Оценката на нивото на сигурност на шемата за електронска идентификација ја оценува телото за оценување на сообразноста кое е акредитирано да врши сертификација по стандарди, определени во подзаконскиот акт од ставот (3) на овој член.

2. Прекугранична соработка во областа на електронската идентификација

Интероперабилност на техничките системи

Член 19

Министерството за информатичко општество и администрација соработува со надлежни меѓународни институции за прашањата поврзани со прекугранична интероперабилност на шемите за електронска идентификација и презема мерки во рамките на својата надлежност со цел да се утврди највисокото ниво на интероперабилност на шемите за електронска идентификација на национално ниво, со цел нивна интеграција и интероперабилност во меѓународно прифатените шеми за електронска идентификација.

Регистрација на шеми за електронска идентификација издадени од странски правни лица

Член 20

(1) Министерството за информатичко општество и администрација може да регистрира во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација и странски правни лица кои се регистрирани на ниво на Европската Унија или во земја членка на унијата, а ги исполнуваат условите утврдени во овој закон.

(2) Министерството за информатичко општество и администрација може да регистрира во Регистарот и шеми за електронска идентификација кои одговараат на високо ниво на сигурност, доколку таа шема се користи од страна на земја членка на Европската Унија.

IV. ДОВЕРЛИВИ УСЛУГИ

1. Општи одредби за доверливи услуги

Вид на доверливи услуги

Член 21

(1) Доверливи услуги се услугите кои се определени како доверливи согласно со одредбите од овој закон.

(2) Квалификувани доверливи услуги се:

- 1) издавање на квалификувани сертификати за електронски потписи;
 - 2) издавање на квалификувани сертификати за електронски печати;
 - 3) издавање на квалификувани сертификати за автентичност на веб страници;
 - 4) квалификувана доверлива услуга на зачувување на квалификувани електронски потписи;
 - 5) квалификувана доверлива услуга на зачувување на квалификувани електронски печати;
 - 6) квалификувана валидација на квалификуван електронски потпис;
 - 7) квалификувана валидација на квалификуван електронски печат;
 - 8) квалификувана доверлива услуга на издавање квалификувани електронски временски печати;
 - 9) квалификувана доверлива услуга на електронска препорачана достава и
 - 10) квалификувана доверлива услуга за електронско складирање на документи.
- (3) Давателот на доверлива услуга или давател на квалификувана доверлива услуга може да обезбеди една или повеќе услуги наведени во ставовите (1) и (2) на овој член.

Одговорност на давателите на доверлива услуга

Член 22

(1) Давател на доверлива услуга е одговорен за штетата која настанала како последица од непостапување во согласност со овој закон, ако штетата е предизвикана намерно или од небрежност.

(2) Товарот за докажување на намерата или небрежноста на давател на доверлива услуга е на физичко или правно лице кое бара надоместок на штета од ставот (1) на овој член.

(3) Кога давателите на доверлива услуга соодветно и однапред ги информираат корисниците на доверливи услуги во однос на ограничувањата за употреба на доверливите услуги кои ги обезбедуваат и кога овие ограничувања се препознатливи за трети страни, давателите на доверливи услуги не се одговорни за штетата која произлегува од користење на услугите кои ги надминуваат наведените ограничувања.

(4) Давателот на квалификувана доверлива услуга треба да биде осигуран од штета или да обезбеди финансиски средства на начин и под условите утврдени од овој закон кои важат за одговорност за штета од употреба на шеми за електронска идентификација.

Одговорност на корисниците на доверливи услуги

Член 23

Корисникот на доверливи услуги е должен да ги чува средствата и податоците за издавање на електронски потпис или печат од неовластен пристап и користење и е должен истите да ги користи во согласност со одредбите на овој закон.

Услови што треба да ги исполнат давателите на доверливи услуги

Член 24

(1) Давателот на неквалификувана доверлива услуга, е должен да го извести Министерството за информатичко општество и администрација за вршење на дејност најдоцна во рок од 15 дена сметано од денот на започнувањето на вршење на дејноста.

(2) Давателот на неквалификувана доверлива услуга е должен во известувањето, покрај основните податоци за правното лице, да ги наведе и видот на услугите, техничките стандарди кои ги применува и изјава дека ќе ги почитува условите за вршење на дејноста.

(3) Министерството за информатичко општество и администрација ги запишува во Регистарот доверливите услуги и давателот на неквалификувана услуга од ставот (2) на овој член, врз основа на поднесеното известување доколку истото ги содржи сите податоци утврдени во ставот (2) на овој член.

(4) Давател на квалификувана доверлива услуга пред да започне да ја врши својата дејност е должен да поднесе барање определено во членот 17 од овој закон за регистрација во Регистарот до Министерството за информатичко општество и администрација.

(5) Давателот на доверлива услуга е должен да ги преземе потребните технички и организациски мерки за управување со ризици кои би можеле да ја загрозат сигурноста при обезбедување на доверливи услуги.

(6) Техничките и организациски мерки обезбедуваат нивото на безбедност да одговара на степенот на ризик, земајќи ги предвид најновите достапни технолошки решенија, а особено се преземаат мерки за спречување и намалување на безбедносни инциденти и да се ограничат штетните ефекти од можните инциденти, како и да се информираат засегнатите страни за негативните ефекти од безбедносните инциденти.

(7) Давателот на доверлива услуга, без одлагање и најдоцна во рок од 24 часа од моментот на дознавањето, ќе го извести надлежниот орган за какви било нарушувања на безбедноста или намалување на интегритетот на услугата кои имаат значително влијание врз обезбедувањето на доверливата услуга или заштитата на личните податоци кои се обработуваат во рамките на обезбедувањето на услугата.

(8) Во случај кога нарушувањето на безбедноста е поврзано со заштитата на личните податоци, давателот на доверлива услуга го известува и надлежниот орган за заштита на личните податоци.

(9) Доколку нарушувањето на безбедноста или губење на интегритетот на доверливата услуга може негативно да влијае на корисниците на доверливите услуги, давателот на доверлива услуга е должен веднаш, а најдоцна во рок од 24 часа да го информира корисникот на доверливата услуга.

(10) Министерството за информатичко општество и администрација ја информира јавноста, директно или со барање до давателот на доверлива услуга да го стори истото, доколку утврди дека со нарушувањето на безбедноста или губењето на интегритетот на доверливите услуги е засегнат јавниот интерес.

(11) Министерството за информатичко општество и администрација соработува со надлежни меѓународни институции во врска со размена на информации за безбедноста и интегритетот на доверливите услуги согласно со меѓународните договори ратификувани согласно со Уставот на Република Северна Македонија.

Надлежност на Министерството за информатичко општество и администрација за доверливи услуги и шеми за електронска идентификација

Член 25

Министерството за информатичко општество и администрација согласно со овој закон ги врши следниве задачи:

1) води Регистар на даватели на доверливи услуги и на шеми за електронска идентификација;

2) ги следи препораките од извештаите за проверка на исполнетост на условите за обезбедување на квалификувана доверлива услуга;

3) врши надзор над работата на давателите на доверливи услуги и издавачите на шеми за електронска идентификација;

4) иницира надзор пред тело за оценување на сообразноста над давателот на доверлива услуга;

5) спроведува вонредна проверка на исполнетост на условите за обезбедување на квалификувани доверливи услуги и шеми, во согласност со закон;

6) соработува со надлежниот орган за заштита на личните податоци и го известува без одлагање ако дознае дека давателите на доверливи услуги не ги почитуваат прописите за заштита на личните податоци;

7) го потврдува постоењето и правилното спроведување на плановите за престанок на вршење на дејност на давателот на доверлива услуга, вклучувајќи го и начинот на кој податоците што ги издал или добил ќе останат достапни со цел да се обезбеди континуитетот на услугата или да послужи како доказ во судска постапка;

8) соработува со органите за супервизија на Европската комисија.

Надлежности на Министерството за информатичко општество и администрација во рамки на прекугранична соработка

Член 26

Министерството за информатичко општество и администрација во рамки на прекуграничната соработка доставува извештаи до Европската комисија за своите активности во согласност со регулативата eIDAS, почнувајќи од датумот на приклучување на Република Северна Македонија како држава во рамки на надлежните органи на ниво на Европската Унија или по пристапување на Република Северна Македонија во Европската Унија.

Надлежно тело за акредитација

Член 27

(1) Министерството за информатичко општество и администрација по претходно мислење од Институтот за акредитација на Република Северна Македонија донесува методологија за акредитација на тела за оценување на сообразност и лаборатории за тестирање на средства која ги вклучува и стандардите определени од страна на министерот за информатичко општество и администрација.

(2) Министерството за информатичко општество и администрација води листа на акредитирани тела за оценување на сообразност и лаборатории во Република Северна Македонија.

(3) Акредитацијата извршена од страна на надлежен орган за акредитација од земја членка на Европската Унија се признава и во Република Северна Македонија.

2. Општи одредби за квалификувани доверливи услуги

Воспоставување на односот меѓу давателот на квалификувана доверлива услуга и корисниците

Член 28

(1) Квалификувана доверлива услуга се обезбедува врз основа на склучен договор меѓу давател на квалификувана доверлива услуга и корисникот на истата, кој договор се склучува по претходно барање од страна на корисникот.

(2) Давателот на квалификувана доверлива услуга, пред склучување на договорот од ставот (1) на овој член, на јасен и недвосмислен начин го известува лицето кое го доставило барањето за користење на квалификувана доверлива услуга за сите важни околности што се однесуваат на користењето на услугата, а особено за:

- 1) прописите и правилата во врска со користењето на квалификувани доверливи услуги;
- 2) било какви ограничувања за користење на квалификувани доверливи услуги и
- 3) мерките што треба да ги преземе корисникот на квалификуваните доверливи услуги и потребната технологија за безбедно користење на квалификувана доверлива услуга.

Услови за обезбедување на квалификувани доверливи услуги

Член 29

(1) Давателот на квалификувана доверлива услуга треба да ги исполни следните услови и тоа:

1) да има вработено лица кои поседуваат потребна стручност, искуство и квалификации за примена на административни и управни постапки, кои ги исполнуваат домашните и меѓународните стандарди и кои поминале обука во областа на информатичката безбедност;

2) да биде осигуран од професионална одговорност за штета или да има обезбедено финансиски средства за надоместок на штета настаната како резултат на обезбедување на квалификувана доверлива услуга;

3) да користи безбедни системи и производи кои се заштитени од неовластени промени и гарантираат техничка сигурност и доверба во процесите што ги поддржуваат;

4) да користи безбедни системи за складирање на податоците што му се доверени, така што податоците треба да се во форма која може да се верификува и тоа:

- дека податоците ќе бидат јавно достапни единствено по претходна согласност од лицето на кого се однесуваат податоците,

- дека само овластени лица можат да прават упис или промена на зачуваните податоци,

- дека податоците можат да бидат подложни на проверка за автентичност.

5) да преземе мерки против фалсификување, кражба и неовластен пристап до податоци;

6) да ги чува и да има можност да ги направи достапни соодветен временски период, дури и по престанокот на вршење на дејноста, сите релевантни информации поврзани со податоците кои се создадени или примени од страна на давателот на квалификувана доверлива услуга, особено за обезбедување на докази во судска постапка и со цел да се обезбеди континуитетот на услугата. Складирањето на овие податоци може да се направи по електронски пат;

7) да чува навремени, точни и добро заштитени бази на податоци за издадените квалификувани електронски сертификати, доколку давателот на квалификувана доверлива услуга издава сертификати;

8) да има ажуриран план за престанок на вршење на дејност со кој ќе обезбеди континуитет во обезбедувањето на квалификувани доверливи услуги за своите корисници;

9) да преземе технички и организациски мерки за обработка на личните податоци во согласност со законите на Република Северна Македонија.

(2) Давателот на квалификувана доверлива услуга е должен да ги донесе следните акти:

- 1) општи услови за обезбедување на услуги кои и се достапни на јавноста;

2) процедури и постапки кои давателот на квалификувана доверлива услуга ги користи за да се обезбеди давање на услуги во согласност со прописите и општите услови наведени во точка 1) од овој став.

(3) Услов за вршење на дејноста давател на квалификувана доверлива услуга е уписот во Регистарот на доверливи услуги и шеми за електронска идентификација.

Осигурување од професионална одговорност

Член 30

Министерот за информатичко општество и администрација го пропишува минималниот износ или видот на покритието на осигурување од ризикот од одговорност за штета причинета од страна на давателот на квалификувана доверлива услуга.

Идентификација на корисникот на квалификувани доверливи услуги

Член 31

(1) Давателот на квалификувана доверлива услуга ги верификува податоците за физичко или правно лице пред издавање на квалификуван сертификат, во согласност со закон.

(2) Проверката на податоците од ставот (1) на овој член давателот на квалификувана доверлива услуга ја врши директно или преку овластено лице во согласност со закон, на следниот начин:

1) преку лично присуство на физичкото лице или на овластениот претставник на правното лице или

2) од далечина, користејќи средства за електронска идентификација, за кои пред издавањето на квалификуваниот сертификат е обезбедено физичко присуство на физичкото лице или на овластен претставник на правното лице и кое ги исполнува условите утврдени во членот 13 од овој закон во однос на нивоата на безбедност на шемата за електронска идентификација соодветни за „значително“ или „високо“ или

3) преку сертификат за квалификуван електронски потпис или за квалификуван електронски печат издаден во согласност со точка 1) или 2) на овој став или

4) преку употреба на други методи за идентификација, признаени на национално ниво, кои обезбедуваат еднаква сигурност во смисла на веродостојност на физичкото присуство. Телото за оценување на сообразноста го потврдува еднаквото ниво на сигурност;

5) со начин за идентификација, употребен во земја членка на Европската Унија.

(3) Во случај на промена на податоците од ставот (1) на овој член, физичкото или правното лице е должно без одлагање, а најдоцна во рок од седум дена сметано од денот на промената, да го извести давателот на квалификувана доверлива услуга за настанатата промена.

(4) За идентификација и користење на квалификувани доверливи услуги, давателот на квалификувана доверлива услуга и издавачот на шеми за електронска идентификација може да изврши верификација користејќи го својот систем или да го интегрира својот систем на интероперабилен начин заради далечинска верификација со централниот регистар на население, документи за лична идентификација, регистри за правни лица и други лица, кога е потребно.

Оценка на условите за обезбедување на квалификувани доверливи услуги

Член 32

(1) Оценување на исполнетоста на условите за обезбедување на квалификувани доверливи услуги врши телото за оценување на сообразноста.

(2) Телото за оценување на сообразност е надлежно и за вршење на проверка на сообразност и за даватели на неквалификувана доверлива услуга, по претходна иницијатива на Министерството за информатичко општество и администрација или по барање на давателот на услугата.

(3) По спроведување на оцената за исполнетост на услови, телото за оцена на сообразност е должно да изготви извештај за оцена на сообразност.

(4) Оценувањето за сообразност задолжително се врши пред почетокот на вршење на дејноста давател на квалификувана доверлива услуга, како и најмалку еднаш на секои 24 месеци, за секој квалификуван давател на доверливи услуги.

(5) По изготвениот извештај за спроведената оцена на сообразност на барателот или давател на квалификувана доверлива услуга, телото за оценување на сообразност извештајот го доставува до Министерството за информатичко општество и администрација, веднаш а најдоцна во рок од три работни дена.

(6) Министерството може да побара итно преоценување на сообразноста ако постојат неправилности во обезбедувањето на квалификувани доверливи услуги или ако настанал инцидент кој значително ја загрозил или нарушил безбедноста на информациите.

(7) Цената на оценување на сообразност, вклучувајќи преоценка за итни случаи, се на товар на давателот на квалификувана доверлива услуга.

(8) Министерот за информатичко општество и администрација утврдува листа на стандарди кои треба да бидат исполнети од страна на телото за оценување на сообразност, потребна содржина на извештајот за оцена на сообразност, постапка за оценување за усогласеност со барањата, како и листа на правни лица кои се овластени во Република Северна Македонија или во земја членка на Европската Унија кои можат да вршат оценување на сообразност во Република Северна Македонија.

Постапка за упис на давател на квалификувана доверлива услуга во Регистарот

Член 33

(1) Правното лице кое има намера да обезбедува квалификувани доверливи услуги поднесува барање до Министерството за информатичко општество и администрација за регистрација во Регистарот, пред да започне да врши дејност давател на квалификувана доверлива услуга.

(2) Во прилог на барањето од ставот (1) на овој член правното лице ги приложува и материјалите наведени како информации во барањето, вклучувајќи го и извештајот за оценување на сообразност во согласност со членот 32 од овој закон.

(3) Министерството за информатичко општество и администрација донесува решение за регистрација на барателот во Регистарот, со кое на давателот на доверливи услуги му доделува статус на давател на квалификувана доверлива услуга, во рок од 60 дена од денот на приемот на барањето, доколку истото е целосно и во зависност од наводите од извештајот за оценување на сообразност.

(4) По исклучок на ставот (3) на овој член, кога се неопходни дополнителни проверки или прибавување на дополнителни докази за кои е потребен подолг рок, Министерството за информатичко општество и администрација ќе го продолжи рокот за донесување на решение за регистрација во Регистарот но не подолго од 60 дена од утврдениот рок од ставот (3) на овој член.

(5) При одлучувањето, Министерството за информатичко општество и администрација може да бара приложување и на дополнителни докази, како и да спроведе дополнителна проверка на техничките и организациски мерки и проверка на безбедносните капацитети на барателот и на услугите, во согласност со закон.

(6) Доколку барателот или услугите наведени во барањето не ги исполнуваат условите пропишани со овој закон, Министерството за информатичко општество и администрација донесува решение за отфрлање на барањето за регистрација во регистарот по истекот на рокот утврден со став (3) или став (4) на овој член.

Престанок на вршење на дејноста давател на квалификувана доверлива услуга

Член 34

(1) Давателот на квалификувана доверлива услуга кој има намера да престане да ја врши оваа дејност е должен за намерата да ги извести корисниците на квалификувани доверливи услуги и Министерството за информатичко општество и администрација, најдоцна три месеци пред планираниот престанок на вршење на дејноста.

(2) Давателот на квалификувана доверлива услуга кој ќе престане да ја врши оваа дејност е должен да обезбеди друг давател на квалификувана доверлива услуга кој ќе продолжи со извршувањето на овие услуги за корисниците на квалификуваните доверливи услуги и за преземените мерки веднаш, односно додека тече рокот определен во ставот (1) на овој член ќе го извести Министерството за информатичко општество и администрација.

(3) Давателот на квалификувана доверлива услуга е должен да ја достави целокупната документација и сите потребни технички средства во согласност со закон, во однос на обезбедување на услуги од страна на друг давател на квалификувана доверлива услуга на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги.

(4) Доколку давателот на квалификувана доверлива услуга не постапи во согласност со обврската утврдена во ставовите (2) и (3) на овој член, Министерството за информатичко општество и администрација ќе побара од давателот на квалификувана доверлива услуга без одлагање до министерството да ја достави целокупната документација и опрема, вклучително и процедурите за постапување со истите.

(5) Министерството привремено ќе ја чува документацијата и опремата, сè до обезбедување на друг давател на квалификувана доверлива услуга кој ќе продолжи да ги извршува овие услуги за корисниците, за сметка на давателот на квалификувана доверлива услуга кој престанува да ја врши оваа дејност.

(6) Начинот и Процедурата за чувањето на документацијата и опремата, ги пропишува министерот за информатичко општество и администрација.

(7) Во случај на привремена забрана за вршење на дејност квалификуван давател на доверливи услуги, квалификуваните сертификати издадени пред денот на стапувањето во сила на забраната, остануваат во важност.

Листа на даватели на квалификувани доверливи услуги

Член 35

(1) Министерството за информатичко општество и администрација ја објавува листа на даватели на квалификувани доверливи услуги, како и листа на квалификувани доверливи услуги кои тие ги обезбедуваат на својата веб страница, во електронска форма која е погодна за автоматска обработка.

(2) Листата од ставот (1) на овој член е потпишана со електронски потпис или запечатена со електронски печат на Министерството за информатичко општество и администрација.

(3) Податоците во листата на даватели на квалификувани доверливи услуги произлегуваат од Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација, како и податоци преземени со користење на автоматски средства.

(4) Формата и начинот на објавување на листата од ставот (1) на овој член ја пропишува министерот за информатичко општество и администрација.

Ознака за доверба на квалификувана доверлива услуга

Член 36

(1) Оznakата за доверба на квалификувана доверлива услуга (во натамошниот текст: како ознака за доверба) е знак кој е едноставен, препознатлив и јасно укажува на квалификувана доверлива услуга, чија форма, содржина и лого се утврдени со ставот (3) на овој член.

(2) Давателите на квалификувани доверливи услуги имаат право да ја користат ознаката за доверба за квалификувана доверлива услуга за која се регистрирани и истата се должни да ја поврзат со листата на квалификувани даватели на доверливи услуги.

(3) Министерот за информатичко општество и администрација ги пропишува формата, структурата, големината и логото на ознаката за доверба на квалификувана доверлива услуга.

Прекугранично признавање на даватели на доверливи услуги

Член 37

(1) На давател на доверлива услуга регистриран со седиште во странска држава му се признава статусот давател на доверливи услуги во Република Северна Македонија доколку истиот е регистриран во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација.

(2) Давателите на доверлива услуга кои се основани од земја членка на Европската Унија и се запишани во Листата на доверливи услуги на Европската Унија, можат да работат и да обезбедуваат услуги на територијата на Република Северна Македонија, без претходна регистрација во Регистарот на даватели на доверливи услуги и шеми за електронска идентификација.

(3) Давателите на квалификувани доверливи услуги регистрирани со седиште во Република Северна Македонија, а кои се регистрирани во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација, се правно еквивалентни на квалификуваните доверливи услуги обезбедени од страна на давателите на квалификувани доверливи услуги основани во Европската Унија, врз основа на претходно склучен договор меѓу Република Северна Македонија и Европската Унија.

(4) Со договорот наведен во ставот (3) на овој член особено се гарантира дека:

(а) барањата применливи за даватели на квалификувани доверливи услуги основани во Европската Унија и за квалификуваните доверливи услуги кои тие ги обезбедуваат, се исполнети од страна на давателите на доверливи услуги во Република Северна Македонија и

(б) квалификуваните доверливи услуги обезбедени од страна на квалификуваните даватели на доверливи услуги основани во Европската Унија, се признати како правно еквивалентни на доверливите услуги обезбедени од страна на давателите на доверливи услуги во Република Северна Македонија.

V. ЕЛЕКТРОНСКИ ПОТПИС И ЕЛЕКТРОНСКИ ПЕЧАТ

1. Напреден електронски потпис

Услови кои треба да ги исполни напредниот електронски потпис

Член 38

Напредниот електронски потпис треба:

- 1) да биде на единствен начин поврзан со потписникот;
- 2) да овозможи идентификација на потписникот;
- 3) да е создаден со податоци за создавање на електронски потпис кои потписникот, со високо ниво на доверба, може да ги користи единствено под сопствена контрола;
- 4) да е поврзан со податоци кои се потпишани на таков начин што секоја подоцнежна измена на истите е воочлива.

2. Напреден електронски печат

Услови кои треба да ги исполни напредниот електронски печат

Член 39

Напредниот електронски печат треба:

- 1) да биде на единствен начин поврзан со создавачот на печатот;
- 2) да овозможи идентификација на создавачот на печатот;
- 3) да е создаден со податоци за создавање на електронски печат кои создавачот на печатот, со високо ниво на доверба, може да ги користи единствено под сопствена контрола;
- 4) да е поврзан со податоците кои ги запечатува на таков начин што секоја подоцнежна измена на истите е воочлива.

3. Содржина на квалификуван сертификат за електронски потпис и печат

Член 40

(1) Стандардите кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат ги пропишува министерот за информатичко општество и администрација.

(2) Покрај стандардите од ставот (1) на овој член кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат, можат да содржат и дополнителни податоци кои нема да влијаат врз интероперабилноста и признавањето на квалификуваниот електронски потпис и квалификуваниот електронски печат.

Правна и доказна сила на квалификуваните сертификати за електронски потпис и печат

Член 41

Квалификуваните сертификати за електронски потпис и печат издадени од квалификуваните даватели на доверливи услуги имаат иста правна и доказна сила како јавните исправи.

Укинување или суспензија на квалификуван сертификат за електронски потпис, за електронски печат и за автентичност на веб страница

Член 42

(1) Давателот на квалификувана доверлива услуга кој го издава квалификуваниот сертификат за електронски потпис, за електронски печат и за автентичност на веб страница е должен да го укине издадениот квалификуван сертификат, доколку:

1) сопственикот на сертификатот за квалификуван електронски потпис, за електронски печат или за автентичност на веб страница поднесе барање за поништување на сертификатот;

2) сопственикот на сертификатот ја загуби деловната способност или престанал да постои или се променети околности кои влијаат на валидноста на сертификатот;

3) утврди дека недостасуваат податоци во сертификатот;

4) утврди дека податоците за создавање на квалификуван електронски потпис, за квалификуван електронски печат или за автентичност на веб страница или системот на давателот на квалификувана доверлива услуга е компромитиран на начин кој влијае врз безбедноста и сигурноста на сертификатите;

5) утврди дека податоците за создавање на електронски потпис, за електронски печат или за автентичност на веб страница или системот преку кој се извршува електронска трансакција се изложени на ризик, на начин кој влијае на сигурноста и безбедноста на електронскиот потпис, електронскиот печат или веб страницата и

6) настане престанок на правно лице, под услови утврдени со закон.

(2) Давателот на доверлива услуга кој го издава квалификуваниот сертификат за електронски потпис, за електронски печат или за автентичност на веб страница го известува корисникот на квалификуваната доверлива услуга за поништување на сертификатот во рок од 24 часа од приемот на барањето или од настанувањето на околностите кои се основ за поништување на сертификатот.

(3) Ако квалификуваниот сертификат за електронски потпис, за електронски печат или за автентичност на веб страница биде укинат после првичното издавање, тогаш ја губи важноста од моментот на укинување и неговиот статус на квалификуван сертификат не може да биде вратен под никакви околности.

(4) Давателите на квалификувани доверливи услуги кои издаваат квалификувани сертификати, на секоја засегната страна и обезбедуваат информации за валидноста, суспензијата или укинувањето на издадените квалификувани сертификати.

(5) Информациите од ставот (4) на овој член се ставаат на располагање на секоја засегната страна најмалку за поединечните сертификати, во секое време и по истекот на периодот на нивната важност, на автоматски начин кој е сигурен, ефикасен и без надоместок.

(6) Корисникот на квалификувана доверлива услуга е должен да побара укинување на издадениот сертификат за квалификуван електронски потпис, за квалификуван електронски печат и за автентичност на веб страница од неговиот издавач во случај на губење, оштетување или загрозување на интегритетот на податоците од сертификатот или доколку настане промена на податоците за креирање сертификати.

(7) Во случај на суспензија на сертификат за квалификуван електронски потпис, за електронски печат и за автентичност на веб страница истиот губи важност за времетраење на периодот на важноста на суспензијата.

(8) Информациите за суспензија и нејзиното времетраење за квалификуван сертификат за електронски потпис, за електронски печат или за автентичност на веб страница или за укинување на истите ќе бидат внесени во базата на податоци на издадени квалификувани сертификати кои се чуваат од страна на давателот на квалификувана доверлива услуга и истите ќе бидат видливи при проверка на статусот на валидност на квалификуван електронски сертификат.

Евиденција на издадени и укинати сертификати за квалификуван електронски потпис, за електронски печат и за автентичност на веб страница

Член 43

(1) Издавачот на квалификувани сертификати за електронски потпис, за електронски печат или за автентичност на веб страница е должен да ја чува целокупната документација за издадените и укинатите квалификувани сертификати за електронски потпис, за електронски печат или за автентичност на веб страница, како и средствата за електронска идентификација и верификација во административни, правни и други процедури, најмалку десет години по истекот на рокот за кој е издаден на сертификатот или по неговото укинување.

(2) Обврската од ставот (1) на овој член се однесува и на суспензија на квалификуваните сертификати за електронски потпис, за електронски печат или за автентичност на веб страница.

(3) Податоците од ставот (1) на овој член може да се чуваат и во електронска форма.

Средства за создавање на квалификуван електронски потпис или квалификуван електронски печат

Член 44

Министерот за информатичко општество и администрација ги пропишува техничките стандарди кои треба да бидат исполнети, како и начинот на создавање на квалификувани електронски потписи или квалификувани електронски печати од страна на давателите на квалификувана доверлива услуга.

Сообразност на средствата за создавање на квалификуван електронски потпис или квалификуван електронски печат

Член 45

(1) Оцена на исполнетост на техничките стандарди што се однесуваат на средствата за издавање на квалификувани електронски потписи или квалификувани електронски печати врши акредитирана лабораторија.

(2) Лабораторијата издава потврда за сообразност на средство за создавање на квалификувани електронски потписи или квалификувани електронски печати и за истото го известува Министерството за информатичко општество и администрација најдоцна во рок од седум дена, сметано од денот на издадената потврда за средствата.

(3) Техничките стандарди кои треба да бидат исполнети, а кои се предмет на оцена на исполнетост на технички барања од страна на овластеното тело се пропишани со актот донесен врз основа на членот 44 од овој закон.

(4) Министерството води листа на средства за создавање на квалификуван електронски потпис или квалификуван електронски печат, врз основа на податоците добиени од потврдите од лабораторијата.

(5) Лабораторијата без одлагање, а најдоцна во рок од седум дена од денот на настаната промена е должна да го известува Министерството за информатичко општество и администрација за издавање или одземање на потврда за сообразност на средствата за создавање на квалификувани електронски потписи и квалификувани електронски печати.

(6) Министерот за информатичко општество и администрација ја пропишува содржината и начинот на водењето на листата од ставот (4) на овој член, начинот на поднесување на барање за регистрација во листата, потребните документи со барањето, како и начинот за регистрација во листата.

(7) Содржината на потврдата за сообразност на средство за создавање на квалификувани електронски потписи или квалификувани електронски печати и начинот на нејзино издавање ја пропишува министерот за информатичко општество и администрација.

(8) Средствата од ставот (1) на овој член кои се сертифицирани во акредитирани лаборатории во земја членка на Европската Унија се признаваат и во Република Северна Македонија.

4. Квалификувана доверлива услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат

Валидација на квалификуван електронски потпис или квалификуван електронски печат

Член 46

(1) Процесот на валидација на квалификуван електронски потпис или квалификуван електронски печат се спроведува со цел да се утврди:

1) дали сертификатот кој се однесува на квалификуван електронски потпис или печат во времето на потпишувањето или создавањето на печатот претставува квалификуван електронски сертификат;

2) дали квалификуваниот сертификат бил издаден од давател на квалификувана доверлива услуга и бил валиден во времето на потпишување или запечатување;

3) дали податоците за валидација на потписот или печатот се соодветни со податоците дадени на засегнатата страна;

4) дали единствениот збир на податоци во квалификуваниот сертификат кои го претставуваат потписникот или создавачот на печатот, кои се дадени на засегнатата страна, се точни;

5) дали во случај на користење на псевдоним во времето на потпишување или запечатување истото и е јасно укажано на засегнатата страна;

6) дали електронскиот потпис или електронскиот печат бил создаден од средство за создавање на квалификуван електронски потпис или квалификуван електронски печат;

7) дали интегритетот на податоците кои се потпишани или запечатени не е компромитиран;

8) дали ги исполнуваат условите пропишани со членовите 38 и 39 од овој закон во времето на потпишување или запечатување.

(2) Системот кој се користи за валидација на квалификуван електронски потпис или на електронски печат на засегнатата страна и го обезбедува точниот резултат на процесот на валидација и ѝ овозможува идентификување на сите проблеми од значење за сигурноста.

Услови за обезбедување на квалификувана услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат

Член 47

(1) Квалификувана услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат може да биде обезбедена единствено од давател на квалификувана доверлива услуга и тоа:

1) процесот за валидација на квалификуван електронски потпис или квалификуван електронски печат е спроведен во согласност со членот 46 од овој закон;

2) на засегнатата страна и овозможува да добие потврда од процесот на валидација на автоматизиран начин, кој е сигурен и ефикасен;

3) дека потврдата од процесот на валидација од точката 2) од овој став е запечатена со напреден електронски печат или потпишана со напреден електронски потпис од давателот на квалификуваната доверлива услуга.

(2) Потврдата за валидација на квалификуван електронски потпис или квалификуван електронски печат издадена од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

(3) Стандардите кои треба да ги содржат потврдите за валидација на квалификуван електронски потпис или квалификуван електронски печат ги пропишува министерот за информатичко општество и администрација.

5. Квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати

Услови за обезбедување на квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати

Член 48

(1) Квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати може да биде обезбедена единствено од давател на квалификувана доверлива услуга кој користи процедури и технологии оспособени да ја продолжат веродостојноста на квалификуваниот електронски потпис или квалификуваниот електронски печат и по истекот на период на важење обезбеден преку користење на технолошки средства.

(2) Стандардите кои треба да ги исполни квалификуваната доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати ги пропишува министерот за информатичко општество и администрација со правилник.

Правно дејство на електронскиот потпис

Член 49

(1) Не може да се оспорува доказната сила на електронскиот потпис само затоа што е употребен во електронски облик или затоа што ги исполнува условите за квалификуван електронски потпис.

(2) Квалификуваниот електронски потпис има иста правна и доказна сила како и своерачниот потпис.

Правно дејство на електронскиот печат

Член 50

(1) Не може да се оспорува доказната сила на електронскиот печат само затоа што е употребен во електронски облик или затоа што ги исполнува условите за квалификуван електронски печат.

(2) Квалификуваниот електронски печат е основа за презумција за интегритетот на податоците и за точноста на потеклото на податоците со кои истиот е поврзан.

6. Електронски временски жиг

Услови кои треба да ги исполни квалификуваниот електронски временски жиг

Член 51

(1) Квалификуваниот електронски временски жиг ги исполнува следните услови:

1) го поврзува датумот и времето со податоците на таков начин што разумно може да се претпостави дека можноста податоците да бидат незабележано променети е исклучена;

2) се заснова на прецизен извор за време поврзан со утврден меѓународен стандард за време;

3) запечатен е со напреден електронски печат или потпишан со напреден електронски потпис од давателот на квалификувана доверлива услуга.

(2) Стандардите кои треба да ги исполнат квалификуваните електронски временски жигови ги пропишува министерот за информатичко општество и администрација.

Правно дејство на електронските временски жигови

Член 52

(1) Не може да се оспорува доказната сила на електронскиот временски жиг само затоа што е употребен во електронски облик или затоа што ги исполнува условите за квалификуван електронски временски жиг.

(2) Квалификуваниот електронски временски жиг е основа за презумција за точноста на датумот и времето кои се означени, како и интегритетот на податоците на кои се однесуваат датумот и времето.

(3) Квалификуваниот сертификат за електронски временски жиг издаден од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

7. Електронска достава

Услови за вршење на квалификувана електронска препорачана достава

Член 53

(1) Квалификуваната електронска препорачана достава ги исполнува следните услови:

- 1) да е обезбедена преку еден или повеќе даватели на квалификувана доверлива услуга;
- 2) да обезбеди високо ниво на сигурност за идентификација на испраќачот;
- 3) да обезбеди идентификација на примачот пред доставата на податоците;
- 4) да обезбеди сигурност во процесот на праќање и примање на податоци преку употреба на напреден електронски потпис или напреден електронски печат на давателот на квалификувана доверлива услуга на таков начин што ќе се спречи можноста при евентуална промена на податоците да останат незабележани;

5) обезбеди сигурна размена на податоци која е соодветна на целите на испраќање и примање на податоци, а преку која ќе може јасно да се определи испраќачот и примачот на податоците;

6) да обезбеди сигурност дека времето и датумот на испраќање, примање и можните промени на податоците е јасно означено преку употреба на електронски временски жиг;

7) да обезбеди сигурност дека се исполнети условите поединечно за секој давател на услуга за електронска препорачана достава во случаите кога податоците се пренесуваат меѓу два или повеќе даватели на услуга за електронска препорачана достава.

(2) Стандардите кои ги содржат потврдите за квалификувана електронска препорачана достава ги пропишува министерот за информатичко општество и администрација.

Правно дејство на електронска препорачана достава

Член 54

(1) Не може да се оспорува доказната сила на податоците испратени или примени преку електронска препорачана достава само затоа што се во електронски облик или затоа што ги исполнуваат условите за квалификувана електронска препорачана достава.

(2) Користењето на квалификувана електронска препорачана достава за примање или праќање на податоци е основа за презумција на интегритетот на тие податоци, испраќањето на истите од утврдениот испраќач, нивниот прием од утврдениот примач, како и точноста на датумот и времето на испраќање и примање на тие податоци означени од давателот на услугата квалификувана електронска препорачана достава.

(3) Потврдата за квалификувана електронска препорачана достава издадена од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

8. Проверка на автентичност на веб страници

Квалификуван сертификат за автентичност на веб страници

Член 55

Стандардите кои треба да ги исполнува квалификуваниот сертификат за автентичност на веб страници ги пропишува министерот за информатичко општество и администрација.

Правна и доказна сила на квалификуваниот сертификат за автентичност на веб страници

Член 56

Квалификуваниот сертификат за автентичност на веб страници издаден од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

9. Електронско складирање на документи

Подготовка на документи за електронско складирање

Член 57

(1) Подготовката на документи за електронско складирање се однесува на:

1) документи кои првично биле создадени во електронска форма погодна за електронско складирање;

2) конверзија на електронски документ во поинаков формат погоден за електронско складирање;

3) дигитализација на документи изворно создадени во форма која не е електронска, погодни за електронско складирање.

(2) Во документот подготвен за електронско складирање, може да бидат вклучени и метаподатоци, по избор на лицето кое врши подготовка на документи за електронско складирање или заради потребите на самиот процес.

Подготовка на документи за сигурносно електронско складирање и квалификувано сигурносно електронско складирање

Член 58

(1) При подготовката на документи за сигурносно електронско складирање треба да бидат исполнети следните услови:

1) обезбеди сигурност дека сите основни елементи на содржината на оригиналниот документ се верно пренесени во документот подготвен за електронско складирање, земајќи ги предвид природата и целта на документот, односно да се зачува интегритет на содржината на документот;

2) обезбеди сигурност дека ќе се зачува употребливоста на оригиналниот документ;

3) обезбеди сигурност дека се вклучени сите елементи на содржината на оригиналниот документ што се од значење за неговата автентичност;

4) обезбеди сигурност за интегритетот на оригиналниот документ, како и за неговите прилози, на начин што се употребени електронски потпис или печат и електронски временски жиг;

5) спроведе контрола на точност и квалитет при процесот на конверзија, со цел да се отстранат секакви грешки кои би можеле да бидат предизвикани од овој процес;

6) се осигура дека за активностите преземени во подготовката на документите за сигурносно електронско складирање се води уредна евиденција.

(2) Доколку пропишаниот рок за чување на документите согласно со закон е подолг од пет години, тогаш документот подготвен за сигурносно електронско складирање треба да биде во формат кој е погоден за долгорочно чување.

(3) Подготовката на документи за квалификувано сигурносно електронско складирање задолжително треба да:

1) обезбеди сигурност дека сите основни елементи на содржината на оригиналниот документ се верно пренесени во документот подготвен за електронско складирање, земајќи ги предвид природата и целта на документот, односно да се зачува интегритет на содржината на документот;

2) обезбеди сигурност дека ќе се зачува употребливоста на оригиналниот документ;

3) обезбеди сигурност дека се вклучени сите елементи на содржината на оригиналниот документ што се од значење за неговата автентичност;

4) обезбеди сигурност дека за интегритетот на оригиналниот документ, како и за неговите прилози, се употребени квалификуван електронски потпис или квалификуван електронски печат и квалификуван електронски временски жиг;

5) спроведе контрола на точност и квалитет при процесот на конверзија, со цел да се отстранат секакви грешки кои би можеле да бидат предизвикани од овој процес;

6) се осигура дека за активностите преземени во подготовката на документите за сигурносно електронско складирање се води уредна евиденција.

(4) Доколку пропишаниот рок за чување на документите согласно со закон е од трајна вредност, тогаш документот подготвен за квалификувано сигурносно електронско складирање треба да биде во формат кој е погоден за долгорочно чување.

(5) Владата, на предлог на Министерството за информатичко општество и администрација ги пропишува поблиските услови за подготовка на документите за електронско складирање и квалификувано електронско складирање и форматите на документите кои се погодни за складирање.

Сигурносно електронско складирање и квалификувано сигурносно електронско складирање на документи

Член 59

(1) Сигурносно електронско складирање на документи кои во нивната оригинална форма содржат електронски потпис или печат, а со цел да се потврди интегритетот и потеклото на овие документи, треба да се подготват на тој начин што за време на нивното складирање се користат востановени процедури и технолошки решенија.

(2) Сигурносно електронско чување на документи кои се изготвени согласно со членот 58 од овој закон, на кои е нанесен електронски потпис или печат и електронски временски жиг на начин определен во членот 58 став 1 точка 4) од овој закон со цел да се потврди интегритетот на оригиналниот документ, како и на неговите прилози, се врши така што во текот на постапката за складирање се користат востановени технолошки решенија.

(3) Квалификувано сигурносно електронско складирање на документи кои во нивната оригинална форма содржат квалификуван електронски потпис или квалификуван електронски печат, а со цел да се потврди интегритетот и потеклото на овие документи, треба да се подготват на тој начин што за време на нивното складирање се користат востановени процедури и технолошки решенија.

(4) Сигурносно електронско чување на документи кои се изготвени согласно со членот 58 од овој закон, на кои е нанесен квалификуван електронски потпис или квалификуван електронски печат и квалификуван електронски временски жиг на начин определен во членот 58 став 2 точка 4) од овој закон со цел да се потврди интегритетот на оригиналниот документ, како и на неговите прилози.

(5) Министерот за информатичко општество и администрација пропишува методологија за имплементација на процедурите и технолошки решенија.

Услуги за електронско складирање и квалификувано електронско складирање на документи

Член 60

(1) Услуги за електронско складирање на документи ги обезбедува давател на доверливи услуги, кој има преземено соодветни технички и организациски мерки преку кои обезбедува сигурност на електронско складирање на документи, согласно со одредбите од овој закон.

(2) Давателот на услуги за електронско складирање на документи може да се ограничи на складирање на документи кои во нивната оригинална форма содржат електронски потпис или печат.

(3) За документ кој се чува во рамките на услугите на електронско складирање на документи постои презумција за верност на оригиналниот документ, за кој давателот на услугата електронско складирање на документи издава соодветен сертификат, согласно со одредбите од овој закон.

(4) Ако документот е зачуван со користење на услугите за електронско складирање на документи, така што периодот на складирање е подолг од пропишаниот период на чување на оригиналниот документ согласно со прописите од областа на архивското работење, тогаш оригиналниот документ може да биде уништен, освен ако не е поинаку определено со закон.

(5) Услуги за квалификувано електронско складирање на документи ги обезбедува давател на квалификувана доверлива услуга, кој има преземено соодветни технички и организациски мерки преку кои обезбедува сигурност на квалификуваното електронско складирање на документи, во согласност со одредбите од овој закон.

(6) Давателот на услуги за квалификувано електронско складирање на документи може да се ограничи на складирање на документи во кои нивната оригинална форма содржат квалификуван електронски потпис или квалификуван електронски печат.

(7) За документ кој се чува во рамките на услугите на квалификувано електронско складирање на документи, во правиот промет се смета за верен на оригиналниот документ, за кој давателот на услугата квалификувано електронско складирање на документи издава соодветен сертификат согласно со одредбите од овој закон.

(8) Ако документот е зачуван со користење на услугите за квалификувано електронско складирање на документи, така што периодот на складирање е подолг од пропишаниот период на чување на оригиналниот документ, тогаш оригиналниот документ може да биде уништен, освен ако не е поинаку определено со закон.

(9) Министерот за информатичко општество и администрација ги пропишува стандардите за електронско складирање и квалификувано електронско складирање на документи.

VI. ЕЛЕКТРОНСКИ ОВЛАСТУВАЊА

Регистар на овластувања

Член 61

(1) За остварување на права по електронски пат преку полномошник пред секое трето лице, властодавецот може да овласти полномошник преку електронски регистар на овластувања.

(2) Овластувањето се издава со користење на електронска идентификација на властодавецот и со потпишување на овластувањето со квалификуван електронски потпис.

(3) Властодавецот ги определува дејствијата за кои ги издава овластувањето, обемот и рокот на важноста на истото.

(4) Давателот на квалификувана доверлива услуга за издавање на квалификуван сертификат за електронски потпис којшто го издал квалификуваниот сертификат за електронски потпис на властодавецот го води регистарот на овластувања.

(5) Лицата од ставот (4) на овој член го потврдуваат секој запис во регистарот со квалификуван електронски печат и квалификуван електронски временски жиг.

(6) Министерот за информатичко општество и администрација ја пропишува содржината и начинот на водење на регистарот и проверката на валидноста на овластувањата.

Писмена форма

Член 62

Овластувањата евидентирани во регистарот на овластувања согласно со членот 61 од овој закон имаат иста правна и доказна сила како писмената форма на нотарски заверените овластувања.

Отповикување на овластувањето

Член 63

Отповикувањето на овластувањето се врши со изјава за отповикување на полномошно, дадена на истиот начин и под истите услови како регистрираното овластување.

Водење, чување и пристап до регистарот на овластувања

Член 64

(1) Регистарот на овластувања нема карактер на јавна книга.

(2) Властодателите, овластените лица и засегнатите страни имаат пристап единствено до податоците кои се однесуваат на соодветното овластување поврзано со нив, од Регистарот на овластувања од членот 61 од овој закон.

VII. НАДЗОР

Надзор над давателите на доверливи услуги и даватели на квалификувана доверлива услуга

Член 65

(1) Надзор над примената на овој закон вршат административните службеници во Министерството за информатичко општество и администрација, по претходно овластување од министерот за информатичко општество и администрација.

(2) Овластените лица од ставот (2) на овој член вршат надзор над исполнетоста на условите утврдени со овој закон и прописите донесени за спроведување на овој закон.

(3) Формата и содржината на записникот и на прекршочниот налог ги пропишува министерот за информатичко општество и администрација.

Обем на овластување за вршење на надзор

Член 66

Лицата од членот 65 од овој закон може да:

- 1) наредат отстранување на неправилностите со определување на рок во кои неправилностите ќе бидат отстранети;
- 2) наредат да се забрани употреба на несоодветна инфраструктура и процедури со определување на рок во кој давателот на доверливата услуга е должен да обезбеди соодветни постапки и соодветна инфраструктура;
- 3) привремено да се забрани обезбедување на услугите, се до моментот на обезбедување на соодветни постапки и инфраструктура од страна на давателот на доверлива услуга;
- 4) наредат привремено одземање на некои или на сите сертификати издадени од страна на давателот на доверливата услуга, доколку постои основано сомневање за несоодветно постапување или фалсификување.

VIII. ПРЕКРШОЧНИ ОДРЕДБИ

Член 67

(1) Со парична казна од 5.000 до 10.000 евра во денарска противвредност ќе се казни давател на квалификувана доверлива услуга - правно лице, ако:

- 1) не ги преземе потребните технички и организациски мерки за управување со ризиците кои ја загрозуваат сигурноста при обезбедување на доверливи услуги;
- 2) без одлагање, а најдоцна во рок од 24 часа од моментот на дознавање, не го известат Министерството за информатичко општество и администрација за секое нарушување на безбедноста или губење на интегритетот, услуги кои имаат значително влијание врз обезбедувањето на доверливите услуги или заштитата на личните податоци кои се обработуваат во рамките на услугите;
- 3) при нарушување на безбедноста или губење на интегритетот на услугите, без одлагање, не го известат корисникот на доверливите услуги, ако постои закана за безбедност или губење на интегритетот на доверливите услуги или ако може да влијае негативно на корисниците на доверливите услуги;
- 4) пред склучувањето на договорот од членот 28 став (1) од овој закон не го известат лицето кое го поднело барањето за користење на квалификувани доверливи услуги за сите релевантни околности кои влијаат на услугата согласно со членот 28 став (2) од овој закон;
- 5) не ги исполнуваат условите од членот 29 од овој закон;
- 6) при издавање на квалификувани сертификати за доверливи услуги не ги проверат информациите за идентитетот на физичко или правно лице содржани во квалификуваниот сертификат, во согласно со членот 31 став (2) од овој закон;
- 7) не ја проверат усогласеноста со условите пред започнувањето на обезбедување квалификувани услуги на доверба или најмалку еднаш на секои 24 месеци;
- 8) пред да започне со вршење на дејноста давател на квалификувана доверлива услуга не е запишан во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација;
- 9) кој има намера да престане да ја врши оваа дејност е должен за намерата да го известат секој корисник на квалификувани доверливи услуги и Министерството за информатичко општество и администрација, најдоцна три месеци пред планираниот престанок на вршење на дејноста;

10) во случај на престанок на вршење на дејноста давател на квалификувана доверлива услуга не ги достави сите потребни технички средства во однос на обезбедување на услуги до друг давател на квалификувана доверлива услуга на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги;

11) во случај на престанок на вршење на дејноста давател на квалификувана доверлива услуга не ја достави целокупната документација и опремата во однос на обезбедување на услуги до друг давател на квалификувана доверлива услуга на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги или до Министерството за информатичко општество и администрација;

12) сертификатите за квалификуван електронски потпис или печат не ги содржат сите податоци наведени во членот 47 став (1) од овој закон;

13) давателот на квалификувана доверлива услуга за издавање на сертификати за квалификуван електронски потпис или печат не ги отповика издадените сертификати во случаите наведени во членот 42 став (1) од овој закон;

14) давателот на квалификувана доверлива услуга за издавање на сертификати за квалификуван електронски потпис или печат не ги извести корисниците на квалификувани доверливи услуги за поништување на сертификатот во рок од 24 часа од приемот на известувањето или појава на околности за кои отповикување сертификат;

15) давателот на квалификувана доверлива услуга за издавање на сертификати за квалификуван електронски потпис или печат не ја зачувува комплетната документација за издадени и одземени сертификати за квалификуван електронски потпис или печат, како и средствата за електронска идентификација и верификација во административни, правни и други процедури, најмалку десет години по истекот на важноста на сертификатот;

16) сигурносното електронско складирање и квалификувано електронско складирање на документи не е спроведено согласно со членот 58 од овој закон.

(2) За прекршокот од ставот (1) на овој член ќе му се изрече парична казна од 1.000 до 5.000 евра во денарска противвредност на одговорното лице на правното лице давател на квалификувана доверлива услуга.

(3) Со парична казна од 5.000 до 10.000 евра во денарска противвредност ќе се казни давателот на неквалификувана доверлива услуга ако не го извести Министерството за информатичко општество и администрација за вршење на дејноста, согласно со членот 24 од овој закон.

(4) За прекршокот од ставот (3) на овој член ќе му се изрече парична казна од 1.000 до 5.000 евра во денарска противвредност на одговорното лице на правното лице давател на неквалификувана доверлива услуга.

Член 68

(1) Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни правно лице корисник на квалификувани доверливи услуги, во случај на промена на податоците наведени во членот 31 став (3) од овој закон, ако не го извести веднаш давателот на квалификувана доверлива услуга.

(2) Со парична казна од 500 до 1.000 евра во денарска противвредност ќе се казни одговорното лице на правното лице корисник на квалификувани доверливи услуги, за прекршокот од ставот (1) на овој член.

(3) Со парична казна од 100 до 300 евра во денарска противвредност ќе се казни физичкото лице корисник на квалификувани доверливи услуги, за прекршокот од ставот (1) на овој член.

Член 69

(1) Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни правно лице кое има регистрирана шема за електронска идентификација, ако:

1) шемата на електронска идентификација не ги исполнува условите од членот 11 од овој закон и

2) не ги преземе потребните технички и организациски мерки за управување со ризиците кои би можеле да ја нарушат сигурноста и безбедноста при обезбедување на овие услуги согласно со членот 18 од овој закон.

(2) Со парична казна од 500 до 1.000 евра во денарска противвредност ќе се казни одговорното лице на правното лице, за прекршокот од ставот (1) на овој член.

Член 70

(1) Со парична казна од 7.000 до 15.000 евра во денарска противвредност ќе се казни правно лице давател на квалификувана доверлива услуга, ако не постапи по наредба на овластеното лице за надзор во рок определен согласно со членот 65 од овој закон.

(2) Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни одговорното лице на правното лице давател на квалификувана доверлива услуга, за прекршокот од ставот 1 на овој член.

Член 71

(1) Со парична казна од 7.000 до 15.000 евра во денарска противвредност ќе се казни јавен орган кој нема да ја признае важноста или ќе ја оспори доказната сила на електронскиот документ изготвен согласно со овој закон или дигитализиран документ создаден согласно со членот 10 од овој закон, само затоа што тоа е електронски документ.

(2) Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни функционерот кој раководи со јавниот орган, односно овластеното лице на правното лице кое врши јавни овластувања доколку ја оспорува доказната сила на електронските документи или документите издадени согласно со овој закон, само затоа што се издадени или употребени во електронски формат.

Член 72

(1) За прекршоците утврдени со овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

IX. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 73

Подзаконските акти чие донесување е утврдено со овој закон ќе се донесат во рок од три месеци од денот на влегувањето во сила на овој закон.

Член 74

(1) Електронските потписи издадени до денот на започнувањето на примената на овој закон, согласно со Законот за податоците во електронски облик и електронски потпис („Службен весник на Република Македонија“ број 34/2001, 6/2002, 98/2008 и 33/15) продолжуваат да важат се до истекот на нивната важност.

(2) Правните лица кои вршеле дејност до денот на започнувањето на примената на овој закон, согласно со Законот за податоците во електронски облик и електронски потпис, со започнувањето на примената на овој закон ќе продолжат да ги издаваат електронските

потписи и ќе ги обезбедуваат услугите согласно со Законот за податоците во електронски облик и електронски потпис („Службен весник на Република Македонија“ број 34/2001, 6/2002, 98/2008 и 33/15).

Член 75

(1) Давателите на доверлива услуга кои вршат дејност врз основа на Законот за податоците во електронски облик и електронски потпис се должни да го усогласат своето работење со одредбите на овој закон во рок од една година, сметано од денот на донесувањето на подзаконските акти определени со овој закон.

(2) Во периодот до усогласување со одредбите на овој закон, давателите на доверлива услуга од ставот (1) на овој член ги обезбедуваат услугите за издавање на сертификати за електронски потписи и временски жигови согласно со Законот за податоците во електронски облик и електронски потпис („Службен весник на Република Македонија“ број 34/2001, 6/2002, 98/2008 и 33/15).

(3) Давателите на доверлива услуга кои вршат дејност врз основа на Законот за податоците во електронски облик и електронски потпис, а кои нема да го усогласат своето работење во рок од една година од денот на донесувањето на подзаконските акти предвидени со овој закон нема да бидат запишани во Регистарот за шеми за електронска идентификација и за доверливи услуги.

Член 76

Овој закон престанува да важи со пристапувањето на Република Северна Македонија во Европската Унија.

Член 77

Со денот на започнувањето на примената на овој закон престанува да важи Законот за податоците во електронски облик и електронски потпис („Службен весник на Република Македонија“ број 34/2001, 6/2002, 98/2008 и 33/15).

Член 78

Овој закон влегува во сила со денот на објавувањето во „Службен весник на Република Северна Македонија“, а ќе започне да се применува во рок од една година од денот на донесувањето на подзаконските акти определени со овој закон.